UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/930,029	08/14/2001	William B. Sweet	00131-000100000	3170

31064 7590 10/10/2008
WIESNER & ASSOCIATES
366 CAMBRIDGE AVENUE
PALO ALTO, CA 94306

EXAMINER	
POPHAM, JEFFREY D	
ART UNIT	PAPER NUMBER
2437	
MAIL DATE	DELIVERY MODE
10/10/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 09/930,029	**Applicant(s)** SWEET ET AL.	
	Examiner JEFFREY D. POPHAM	**Art Unit** 2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 April 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22 and 52-67* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22 and 52-67* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *30 November 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

Remarks

Claims 1-22 and 52-67 are pending.

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 4/16/2008 has been entered.

Claim Objections

2. Claims 66 and 67 are objected to because of the following informalities: Claims 66 and 67 are duplicate claims, and one should be canceled. Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

3. Claims 4-6, 15-22, 57, 58, and 63 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s)

contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. Claim 4 recites in the final limitation that the working key will allow the network user to "decrypt other than the selected portions of the encrypted object." There is no basis in the specification for this “other than” portion of the claim. Indeed, this working key is generated for the selected portions, and not for some portions that are unknown.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

4. Claims 52-58 rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claim 52 purports to be a system, however, has no inherently physical components. As an example, the claim recites in (d) "a set of client systems", however, the current specification teaches that a client system may be a browser (page 49, line 23 to page 50, line 8). Without getting into the specifics of each limitations, it appears that each limitation could be purely software, which would make claim 52 a system of software, per se, which is not statutory. In order to be statutory, the claim must include a physical component as a limitation in the claim. The claims dependent upon claim 52 have the same issue.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-20, 52-57, and 59-67 rejected under 35 U.S.C. 103(a) as being unpatentable over Scheidt (U.S. Patent 6,490,680) in view of He (U.S. Patent 6,088,451) and Shanton (U.S. Patent 5,680,452).

Regarding Claim 1,

> Scheidt discloses a method for providing cryptographic capabilities to a plurality of network users over a network, the method comprising:
>
> An access permission security profile that gives the network user the ability to access one or more objects associated with a domain according to the network user's membership in one or more groups within the domain (Column 7, line 59 to Column 8, line 9; and Column 8, line 63 7to Column 9, line 65);
>
> Authenticating the network user according to an n-factor authentication suitable to the plurality of network users and verifying membership in the domain and the one or more groups (Column 7, lines 29-43; and Column 14, lines 24-38);
>
> Creating the access permission security profile having an ephemeral cryptographic characteristic and derived from a combination of the user's membership in the one or more groups (Column 8, line 46 to

Column 10, line 25; and Column 10, lines 53-67), wherein the combination of the user's membership in the one or more groups can be used to form a cryptographic key for enabling the network user to decrypt selected portions of an encrypted object when one or more groups associated with the encrypted object match the network user's membership in one or more groups within the domain (Column 10, line 53 to Column 11, line 12; and Column 17, lines 15-65) and to encrypt selected portions of a plaintext object to be accessed by other network user when the other network users' membership in one or more groups within the domain also match the one or more groups associated with the selected portions of the plaintext object being encrypted (Column 10, line 53 to Column 11, line 12; and Column 16, line 11 to Column 17, line 14); and

Securely transmitting the access permission security profile to the network user over the network wherein the ephemeral cryptographic characteristic allows the network user in receipt of the access permission security profile to perform cryptographic operations for a predetermined period of time (Figure 6; Column 4, lines 7-14; Column 8, line 46 to Column 10, line 25; and Column 10, line 53 to Column 11, line 12);

But does not explicitly disclose that the network is a decentralized public network or receiving a request for an access permission security profile and authenticating such request, or providing access to different portions of an object to different entities accessing the same object (though this is not necessarily claimed).

He, however, discloses that the network is a decentralized public network (Figure 10; and Column 30, lines 47-67);

Receiving a request for an access permission security profile on behalf of a network user (Column 18, line 33 to Column 19, line 15; and Column 25, lines 21-64); and

Authenticating the request from the network user (Column 18, line 33 to Column 19, line 15; and Column 25, lines 21-64). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the security system of He into the access control system of Scheidt in order to provide a mechanism by which a user can request creation and/or transmission of his or her security profile while ensuring that the user is authentic and authorized before sending such profile, such that the profile can be stored securely on a central server and accessed by the user from a variety of different devices.

Shanton, however, discloses providing different access control to portions of objects, such that an different portions of an object may be accessed differently by each entity authorized to access the object (Abstract; Column 8, lines 1-26; and Column 14, lines 7-32). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the embedded object protection system of Shanton into the access control system of Scheidt as modified by He in order to allow the system to be more flexible and offer still more protection, as well as to provide the ability to distribute the same object to many users, while allowing each user to have access to a personalized subset of the embedded object.

Regarding Claim 2,

Scheidt as modified by He and Shanton discloses the method of claim 1, in addition, Scheidt discloses that the creating step comprises:

Identifying one or more groups of network users who are to be provided with cryptographic capabilities according to each network user's membership in a particular combination of groups within the domain (Column 4, line 51 to Column 5, line 2; Column 10, line 53 to Column 11, line 12; and Column 16, line 11 to Column 17, line 14);

Establishing one or more access codes for each group in the domain, wherein each access code is adapted to be combined with other components to form the cryptographic key (Column 4, line 51 to Column 5, line 2; Column 8, lines 31-44; and Column 10, line 53 to Column 11, line 12); and

Creating one or more access permission security profiles for each network user based on membership in one or more different combination of groups in the domain, wherein the access permission security profile for each network user contains at least one access code in correspondence with the network user's membership in at least one group in the domain (Column 8, line 46 to Column 10, line 25; and Column 10, lines 53-67).

Regarding Claim 3,

Scheidt as modified by He and Shanton discloses the method of claim 1, in addition, Scheidt discloses that each group is a category, organization, organizational unit, set of role based credentials, work project, geographical location, or workgroup within the domain (Column 8, lines 31-44).

Regarding Claim 4,

Scheidt discloses a method for providing decryption capabilities to a plurality of network users over a network, the method comprising:

Decryption capabilities associated with a network user that gives the network user the ability to decrypt one or more encrypted objects associated with a domain according to the network user's membership in one or more groups within the domain (Column 7, line 59 to Column 8, line 9; and Column 8, line 63 to Column 9, line 65);

Authenticating the network user according to an n-factor authentication suitable to the plurality of network users and verifying membership in the domain and the one or more groups (Column 7, lines 29-43; and Column 14, lines 24-38);

Creating an access permission security profile derived from a combination of the user's membership in the one or more groups, wherein the combination of the user's membership in the one or more groups can be used to form a cryptographic key and decrypt selected portions of the one or more encrypted objects (Column 8, line 46 to Column 10, line 25; and Column 10, lines 53-67);

Receiving information associated with the selected portions of an encrypted object (Column 10, lines 45-67; Column 16, line 34 to Column 17, line 36);

Generating a cryptographic working key using the cryptographic key associated with the access permission security profile and the received information associated with the selected portions of the encrypted object (Column 10, lines 45-67; Column 16, line 34 to Column 17, line 36); and

Securely transmitting the cryptographic working key to the network user over the network allowing the network user to decrypt the selected portions of the encrypted object (Column 10, lines 45-67; Column 16, line 34 to Column 17, line 36);

But does not explicitly disclose that the network is a decentralized public network or receiving a request for decryption capabilities and authenticating such request, or providing access to different portions of an object to different entities accessing the same object (though this is not necessarily claimed).

He, however, discloses that the network is a decentralized public network (Figure 10; and Column 30, lines 47-67);

Receiving a request for an decryption capabilities on behalf of a network user (Column 18, line 33 to Column 19, line 15; and Column 25, lines 21-64); and

Authenticating the request from the network user (Column 18, line 33 to Column 19, line 15; and Column 25, lines 21-64). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the security system of He into the access control system of Scheidt in order to provide a mechanism by which a user can request creation and/or transmission of his or her security profile while ensuring that the user is authentic and authorized before sending such profile, such that the profile can be stored securely on a central server and accessed by the user from a variety of different devices.

Shanton, however, discloses providing different access control to portions of objects, such that an different portions of an object may be accessed differently by each entity authorized to access the object (Abstract; Column 8, lines 1-26; and Column 14, lines 7-32). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the embedded object protection system of Shanton into the access control system of Scheidt as modified by He in order to allow the system to be more flexible and offer still more protection, as well as to provide the ability to distribute the same object to many users, while allowing each user to have access to a personalized subset of the embedded object.

Regarding Claim 5,

Scheidt as modified by He and Shanton discloses the method of claim 4, in addition, Scheidt discloses that the creating step comprises:

Identifying one or more groups of network users who are to be provided with cryptographic capabilities according to each network user's membership in a particular combination of groups within the domain (Column 4, line 51 to Column 5, line 2; Column 10, line 53 to Column 11, line 12; and Column 16, line 11 to Column 17, line 14);

Establishing one or more access codes for each group in the domain, wherein each access code is adapted to be combined with other components to form the cryptographic key (Column 4, line 51 to Column 5, line 2; Column 8, lines 31-44; and Column 10, line 53 to Column 11, line 12); and

Creating one or more access permission security profiles for each network user based on membership in one or more different combination of groups in the domain, wherein the access permission security profile for each network user contains at least one access code in correspondence with the network user's membership in at least one group in the domain (Column 8, line 46 to Column 10, line 25; and Column 10, lines 53-67).

Regarding Claim 6,

Scheidt as modified by He and Shanton discloses the method of claim 4, in addition, Scheidt discloses that each group is a category, organization, organizational unit, set of role based credentials, work project, geographical location, or workgroup within the domain (Column 8, lines 31-44).

Regarding Claim 7,

Scheidt discloses a method for cryptographically securing the distribution of information over a network to a plurality of network users, the method comprising:

Creating a computer representable data object (Column 4, line 51 to Column 5, line 2);

Associating a pseudorandom cryptographic key with the data object (Column 7, lines 44-58; Column 10, lines 45-67; and Column 16, line 11 to Column 17, line 14);

Encrypting the object using a working key derived from the pseudorandom cryptographic key associated with the object and other components (Column 7, lines 44-58; Column 10, lines 45-67; and Column 16, line 11 to Column 17, line 14);

Creating a set of one or more access permission credentials that identify the roles each of the plurality of network users may possess in a domain and their membership in one or more groups as defined by various combinations of the one or more access permission credentials (Column 8, line 46 to Column 10, line 25; and Column 10, lines 53-67);

Assigning a member credential to the object, wherein the member credential is a specific combination of the one or more access permission credentials ensuring that only network users having a matching member credential are able to decrypt the data object (Column 16, line 11 to Column 17, line 50);

Inserting the pseudorandom cryptographic key in a header of the object after first encrypting the pseudorandom cryptographic key with a credential key derived from the member credential associated with the object (Column 16, line 11 to Column 17, line 14);

Transmitting the data object over the network having the encrypted pseudorandom key inserted in a portion of the object (Column 16, line 11 to Column 17, line 14); and

Securely transmitting an access permission security profile, having an ephemeral cryptographic characteristic, to at least one network user from the plurality of network users wherein the access permission security profile for the at least one network user can be used to generate a credential key capable of decrypting the encrypted pseudorandom cryptographic key associated with the encrypted object because the member credential of the network user matches the member credentials associated with the encrypted object, wherein the ephemeral cryptographic characteristic allows the network user in receipt of the access permission security profile to perform cryptographic operations for a predetermined period of time (Figure 6; Column 4, lines 7-14; Column 8, line 46 to Column 10, line 25; and Column 10, line 53 to Column 11, line 12);

But does not explicitly disclose that the network is a decentralized public network or the usage of embedded objects within an object.

He, however, discloses that the network is a decentralized public network (Figure 10; and Column 30, lines 47-67). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the security system of He into the access control system of Scheidt in order to provide a mechanism by which a user can request creation and/or transmission of his or her security profile while ensuring that the user is authentic and authorized before sending such profile, such that the profile can be stored securely on a central server and accessed by the user from a variety of different devices.

Shanton, however, discloses including one or more embedded objects in a data object (Abstract; Column 8, lines 1-42; and Column 9, line 63 to Column 10, line 10);

Associating a pseudorandom key with each of the one or more embedded objects of the data object (Abstract; Column 8, lines 1-42; and Column 14, lines 7-32);

Encrypting each of the embedded objects using a working key derived from the pseudorandom cryptographic key associated with the embedded object and other components (Abstract; Column 8, lines 1-42; and Column 14, lines 7-32);

Assigning a member credential to each of the selected embedded objects so that only a user with a matching credential can decrypt encrypted embedded objects of the object (Abstract; Column 8, line 1-42 to Column 9, line 23; and Column 14, lines 7-32); and

Inserting a pseudorandom key in a header of each embedded object (Abstract; Column 6, lines 7-39; Column 8, lines 1-42; and Column 14, lines 7-32). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the embedded object protection system of Shanton into the access control system of Scheidt as modified by He in order to allow the system to be more flexible and offer still more protection, as well as to provide the ability to distribute the same object to many users, while allowing each user to have access to a personalized subset of the embedded object.

Regarding Claim 8,

Scheidt as modified by He and Shanton discloses the method of claim 7, in addition, Scheidt discloses that the information is digital content (Column 7, lines 12-27).

Regarding Claim 9,

Scheidt as modified by He and Shanton discloses the method of claim 7, in addition, He discloses that securely transmitting further includes receiving a request for an access permission security profile on behalf of a network user and authenticating the request from the network user (Column 18, line 33 to Column 19, line 15; and Column 25, lines 21-64); and Scheidt discloses authenticating users using an n-factor authentication suitable to authenticate the plurality of network users (Column 7, lines 29-43; and Column 14, lines 24-38).

Regarding Claim 10,

Scheidt as modified by He and Shanton discloses the method of claim 7, in addition, He discloses that securely transmitting further includes sending a request for an access permission security profile on behalf of a network user to a centralized server system over the network; receiving the request on behalf of the network user at the central server system; and authenticating the request as from the network user (Column 18, line 33 to Column 19, line 15; and Column 25, lines 21-64); and Scheidt discloses authenticating users using an n-factor authentication suitable to authenticate the plurality of network users (Column 7, lines 29-43; and Column 14, lines 24-38).

Regarding Claim 11,

Scheidt as modified by He and Shanton discloses the method of claim 7, in addition, Scheidt discloses that the step of securely transmitting an access permission security profile is not performed if the user already has possession of an access permission security profile (Figure 6; Column 4, lines 7-14; Column 8, line 46 to Column 10, line 25; and Column 10, line 53 to Column 11, line 12).

Regarding Claim 12,

Scheidt as modified by He and Shanton discloses the method of claim 7, in addition, Scheidt discloses that the working key may further be derived from at least a domain component, a maintenance component, and the pseudorandom key (Column 7, lines 44-58; Column 10, line 45 to Column 11, line 12; and Column 16, line 11 to Column 17, line 14).

Regarding Claim 13,

Scheidt as modified by He and Shanton discloses the method of claim 10, in addition, Scheidt discloses that the creating step comprises:

Identifying one or more groups of network users who are to be provided with cryptographic capabilities (Column 4, line 51 to Column 5, line 2; Column 10, line 53 to Column 11, line 12; and Column 16, line 11 to Column 17, line 14);

Establishing one or more access codes for each group, wherein each access code is adapted to be combined with other components to form a cryptographic key (Column 4, line 51 to Column 5, line 2; Column 8, lines 31-44; and Column 10, line 53 to Column 11, line 12); and

Creating one or more access permission security profiles for each network user based on membership in one or more different combination of groups in the domain, wherein the access permission security profile for each network user contains at least one access code in correspondence with the network user's membership in at least one group in the domain (Column 8, line 46 to Column 10, line 25; and Column 10, lines 53-67).

Regarding Claim 14,

Scheidt as modified by He and Shanton discloses the method of claim 13, in addition, Scheidt discloses that each group is a category, organization, organizational unit, set of role based credentials, work project, geographical location, or workgroup within the domain (Column 8, lines 31-44).

Regarding Claim 15,

Scheidt as modified by He and Shanton discloses the method of claim 1, 4, or 9, in addition, He discloses that the request is initiated in-band by the network user over the network (Column 18, line 33 to Column 19, line 15; and Column 25, lines 21-64).

Regarding Claim 16,

Scheidt as modified by He and Shanton discloses the method of claim 1, 4, 9, 10, or 11, in addition, Scheidt discloses that the access permission security profile is in the form of a token that is adaptable to expire (Column 8, line 46 to Column 10, line 25; and Column 10, lines 53-67).

Regarding Claim 17,

Scheidt as modified by He and Shanton discloses the method of claim 1, 4, 9, or 10, in addition, Scheidt discloses that the authenticating step includes the use of biometric identification (Column 12, line 46 to Column 13, line 19).

Regarding Claim 18,

Scheidt as modified by He and Shanton discloses the method of claim 1, 4, 9, or 10, in addition, Scheidt discloses that the authenticating step includes the use of a hardware token (Column 11, lines 22-30; and Column 11, line 65 to Column 12, line 46).

Regarding Claim 19,

Scheidt as modified by He and Shanton discloses the method of claim 1, 4, 9, or 10, in addition, Scheidt discloses that the authenticating step includes the use of a software token (Column 14, lines 30-45).

Regarding Claim 20,

Scheidt as modified by He and Shanton discloses the method of claim 1, 4, 9, or 10, in addition, Scheidt discloses that the authenticating step includes the use of a user password (Column 11, lines 14-20).

Regarding Claim 52,

Scheidt discloses a centralized security management system for distributing cryptographic capabilities to a plurality of network users over a network, the system comprising:

A plurality of member tokens for providing cryptographic capabilities to authenticated users of the network (Column 7, line 59 to Column 8, line 9; and Column 8, line 63 to Column 9, line 65);

A set of server systems for managing the distribution of the member tokens (Column 7, line 13 to Column 9, line 24);

A set of client systems, wherein each client system includes means for receiving a member token and means for utilizing the cryptographic capabilities provided by the member token for selective encryption and decryption (Figure 6; Column 4, lines 7-14; Column 8, line 46 to Column 10, line 25; and Column 10, line 53 to Column 11, line 12); and

Means for securely distributing a member token from at least one server system to at least one client system over the network (Figure 6; Column 4, lines 7-14; Column 8, line 46 to Column 10, line 25; and Column 10, line 53 to Column 11, line 12);

But does not explicitly disclose that the network is a decentralized public network, means for requesting a member token from at least one server system, or providing access to different portions of an object to different entities accessing the same object (though this is not necessarily claimed).

He, however, discloses that the network is a decentralized public network (Figure 10; and Column 30, lines 47-67); and

Means for requesting a member token from at least one server system (Column 18, line 33 to Column 19, line 15; and Column 25, lines 21-64). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the security system of He into the access control system of Scheidt in order to provide a mechanism by which a user can request creation and/or transmission of his or her security profile while ensuring that the user is authentic and authorized before sending such profile, such that the profile can be stored securely on a central server and accessed by the user from a variety of different devices.

Shanton, however, discloses providing different access control to portions of objects, such that an different portions of an object may be accessed differently by each entity authorized to access the object (Abstract; Column 8, lines 1-26; and Column 14, lines 7-32). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the embedded object protection system of Shanton into the access control system of Scheidt as modified by He in order to allow the system to be more flexible and offer still more protection, as well as to provide the ability to distribute the same object to many users, while allowing each user to have access to a personalized subset of the embedded object.

Regarding Claim 53,

Scheidt as modified by He and Shanton discloses the system of claim 52, in addition, Scheidt discloses that each client system further includes user authentication means (Column 11, lines 14-40).

Regarding Claim 54,

Scheidt as modified by He and Shanton discloses the system of claim 52, in addition, He discloses that the means for requesting a member token resides on each client system (Column 18, line 33 to Column 19, line 15; and Column 25, lines 21-64).

Regarding Claim 55,

Scheidt as modified by He and Shanton discloses the system of claim 52, in addition, Scheidt discloses that means for authenticating a user resides on at least one server system (Column 7, lines 13-58; and Column 13, lines 22-36).

Regarding Claim 56,

Scheidt as modified by He and Shanton discloses the system of claim 52, in addition, Scheidt discloses that managing the distribution of the member tokens includes dynamic updating of the member tokens (Column 8, line 46 to Column 10, line 25).

Regarding Claim 57,

Scheidt as modified by He and Shanton discloses the method of claim 1, 4, 7, or the system of claim 52, in addition, He discloses that the decentralized public network is the Internet (Figure 10; and Column 30, lines 47-67).

Regarding Claim 59,

Scheidt as modified by He and Shanton discloses the method of claim 1, in addition, Scheidt discloses that the access permission security profile received by the network user remains encrypted on a persistent memory device until decryption of one or more portions of the access permission security profile is deemed necessary to effectuate performing one or more cryptographic operations on one or more objects (Column 7, lines 44-58; Column 10, line 45 to Column 11, line 12; and Column 16, line 11 to Column 17, line 65).

Regarding Claim 60,

Scheidt as modified by He and Shanton discloses the method of claim 59, in addition, Scheidt discloses that the access permission security profile may be decrypted when the network user in receipt of the access permission security profile successfully performs an n-factor authentication operation (Column 7, lines 44-58; Column 10, line 45 to Column 11, line 12; and Column 16, line 11 to Column 17, line 65).

Regarding Claim 61,

Scheidt as modified by He and Shanton discloses the method of claim 1, in addition, Scheidt discloses that the network user in receipt of the access permission security profile can no longer perform cryptographic operations on one or more objects when the predetermined period of time associated with the ephemeral cryptographic characteristic has expired (Column 8, line 46 to Column 10, line 25; and Column 10, lines 53-67).

Regarding Claim 62,

Scheidt as modified by He and Shanton discloses the method of claim 1, in addition, Scheidt discloses that the network user in receipt of the access permission security profile can not perform cryptographic operations on one or more objects when one or more groups associated with the encrypted object do not match the network user's membership in one or more groups within the domain (Column 8, line 46 to Column 10, line 25; and Column 10, lines 53-67).

Regarding Claim 63,

Scheidt as modified by He and Shanton discloses the method of claim 1, in addition, Scheidt discloses that decrypting selected portions of the encrypted object with the access permission security profile produces a secondary cryptographic key to be used in further decrypting the selected portions of the encrypted object (Column 7, lines 44-58; Column 10, line 45 to Column 11, line 12; and Column 16, line 11 to Column 17, line 65).

Regarding Claim 64,

Scheidt as modified by He and Shanton discloses the method of claim 1, in addition, Scheidt discloses that encrypting selected portions of the plaintext object includes encrypting a randomly generated value with respect to the one or more groups associated with plaintext object to be encrypted (Column 7, lines 44-58; Column 10, line 45 to Column 11, line 12; and Column 16, line 11 to Column 17, line 14).

Regarding Claim 65,

Scheidt as modified by He and Shanton discloses the method of claim 2, in addition, Scheidt discloses that the network user's membership in one or more different combination of groups corresponds to member credentials associated with the network user and selected from a set of access permission credentials associated with the domain (Column 4, line 51 to Column 5, line 2; Column 10, line 53 to Column 11, line 12; and Column 16, line 11 to Column 17, line 14).

Regarding Claim 66,

Scheidt as modified by He and Shanton discloses the method of claim 65, in addition, Scheidt discloses that encrypting selected portions of the plaintext object includes encrypting the plaintext object using a randomly generated value (Column 7, lines 44-58; Column 10, line 45 to Column 11, line 12; and Column 16, line 11 to Column 17, line 14);

Generating a pseudorandom value by encrypting the randomly generated value in combination with one or more different credentials selected from the set of access permission credentials associated with the domain (Column 7, lines 44-58; Column 10, line 45 to Column 11, line 12; and Column 16, line 11 to Column 17, line 14); and

Embedding the pseudorandom value in the selected portions of the encrypted plaintext object (Column 7, lines 44-58; Column 10, line 45 to Column 11, line 12; and Column 16, line 11 to Column 17, line 14).

Regarding Claim 67,

Claim 67 is the exact same claim as claim 66 and is rejected for the same reasons.

6. Claims 21 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Scheidt in view of He and Shanton, further in view of Win (U.S. Patent 6,161,139).

Regarding Claim 21,

Scheidt as modified by He and Shanton may not explicitly disclose that the authenticating step includes the use of a record of time at which the request was made.

Win, however, discloses that the authenticating step includes the use of a record of time at which the request was made (Column 9, lines 46-52; and Column 15, lines 46-60). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the RBAC system of Win into the access control system of Scheidt as modified by He and Shanton in order to detect login anomalies and take action against such anomalies in order to further protect against unauthorized access.

Regarding Claim 22,

Scheidt as modified by He and Shanton may not explicitly disclose that the authenticating step includes the use of a record of the user's physical location.

Win, however, discloses that the authenticating step includes the use of a record of the user's physical location (Column 9, lines 46-52; and Column 15, lines 46-60). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the RBAC system of Win into the access control system of Scheidt as modified by He and Shanton in order to detect login anomalies and take action against such anomalies in order to further protect against unauthorized access.

7. Claim 58 is rejected under 35 U.S.C. 103(a) as being unpatentable over Scheidt in view of He and Shanton, further in view of Anderson (U.S. Patent 5,805,674).

Scheidt as modified by He and Shanton does not explicitly disclose that the decentralized public network is a cellular phone network.

Anderson, however, discloses that the decentralized public network is a cellular phone network (Column 11, line 62 to Column 12, line 3). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the cell phone security system of Anderson into the access control system of Scheidt as modified by He and Shanton in order to allow the system to increase a level of authentication in response to suspicious events (such as, by requiring biometrics where a password would normally suffice).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JEFFREY D. POPHAM whose telephone number is (571)272-7215. The examiner can normally be reached on M-F 9:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571)272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Jeffrey D Popham
Examiner
Art Unit 2437

/Jeffrey D Popham/
Examiner, Art Unit 2437

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437